UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/808,720	03/15/2001	Hakon Gudbjartsson	2345.2003-001	5511

21005 7590 04/05/2005

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/808,720	GUDBJARTSSON ET AL.	
	Examiner	Art Unit	
	Paula W Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/10/2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7-23 and 25-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7-23 and 25-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 12/10/04. Original application contained Claims 1-39. Applicant cancelled Claims 5, 6, and 24, and amended Claims 1, 7, and 20. The amendment filed on 12/10/04 have been entered and made of record. Therefore, presently pending claims are 1-4, 7-23, and 25-39.

Response to Arguments

Applicant's arguments filed 12/10/04 have been fully considered but they are not persuasive because of following reasons.

Applicant argued Spelman does not disclose not suggest the use of a secret sharing module to control access to a mapping module that maps identifiers from one domain to another. This is not found persuasive. Spelman discloses a recryptor 30 in combination with directory 35. Access control to the mapping function of the recryptor is performed by authentication of the user's using digital signature (column 6 line 65 and column 7 line 25).

Applicant argues further that Spelman does not however disclose or suggest the use or secret sharing to control access to any mapping that is used between any of the parties. This is not found persuasive because the applicant does not claim the use of secret sharing to control access to any mapping. The applicant claims "a secret sharing module for controlling access to the mapping module. Although the secret sharing module controls access to the mapping module, the applicant does not claim that the secret sharing module performs secret sharing.

Applicant argues further that the Spellman does not disclose or suggest that the recryptor 30 requires entry of multiple keyholder passwords, or uses another secret sharing technique, in its operation. This is not found persuasive because the applicant does not claim requiring multiple key holder passwords. Although claim 20 claims controlling access to the mapping using secret sharing, the applicant does not claim the secret sharing operations used for access control. The recryptor of Spelman discloses access control using secret sharing using GSO key and stream cipher keys (page 8 lines 3-9).

Applicant argues further that Spelman does not handle data that can be split into identifier portion and a research portion. However, Spelman does indeed teach an identifier portion, the merchants name, and a research portion the consumer information (column 6 lines 49-55). The definition of research information is collecting information about a subject. Spelman discloses colleting information about the consumer.

Further the Spelman discloses the merchant and the consumer that are obviously in different domains. It is inherent that these participators are in two different domain because if they were in the same domain there would be no need for the system, since they would be trusted members.

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the

examiner asserts that Spelman does teach or suggest the subject matter broadly recited in independent Claims 1, 7, and 20. Dependent Claims 2-4, 8-19, 21-23, and 25-39 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action. Accordingly, rejections for claims 1-4, 8-23, and 25-39 are respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 7-8, 16-19, 20-21, 25-26, 34-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman.

In reference to claims 1 and 20, Spelman discloses a method of exchanging encrypted information with a merchant without having the merchant's key (column 1 lines 4-29). The method comprises a communication module for establishing a communication connection between a sender and a receiver (Fig. 1); a mapping module coupled to the communication module for mapping working data of the sender to working data of the receiver (Fig. 1 part 30); the working data having an identifier portion (Fig. 2D merchant name) and a research data portion (Fig. 2D GSO). The mapping module maps between the identifier portion of the working data in the one domain to the identifier portion of the working data in the different domain. The recryptor uses the merchant name to fine the public key of the merchant, M, to re-

encrypt the blob 1 (Fig. 3). Spelman discloses a recryptor 30 in combination with directory 35. Access control to the mapping function of the recryptor is performed by authentication of the user's using digital signature (column 6 line 65 and column 7 line 25).

Although Spelman does not expressly disclose the receiver and the sender being in different domains, Spelman does disclose that the sender being a customer and the merchant acquirer being an organization such as a bank (column 4 lines 19-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art for the customer, the merchant, and the merchant acquire being in the different domains. One of ordinary skill in the art would have been motivated to do this because the advent of the Internet enabled customers to purchase, securely, services and products remotely over the Internet.

In reference to claims 2 and 21, a system is disclosed wherein the research data portion of the working data includes personal data of individuals (column 5 lines 63-65).

In reference to claims 7 and 25, Spelman does not expressly disclose permanent storage means for storing data in a tamper-proof manner.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store data in a permanent storage means for storing data in a tamper-proof manner. One of ordinary skill in the art would have been motivated to do this because it would discourage fraudulent activities.

In reference to claims 8 and 26, wherein the permanent storage means encrypts non-queried parts of the data, said encryption using an encryption key, and the secret sharing module storing the encryption key (Fig. 2D).

In reference to claims 16 and 34, wherein the sender and receiver are respectively one of a software implementation and a human being. Spelman states that each block in Fig. 1 represents varying computing devices; therefore it can include software and a human being (column 4 lines 43-58).

In reference to claims 17 and 35, wherein collection of the sender and receiver is in respective different sessions. Spelman discloses a system wherein the customer sends information to the merchant and then the merchant sends the information to the recryptor (Fig. 1). This suggests different sessions.

In reference to claims 18 and 36, wherein the communication module further enables communication connection by a supervisor in addition to the sender and receiver. The system of Spelman discloses a merchant acquirer (Fig. 1). This suggests a third party involved in the communications.

In reference to claims 19 and 37 wherein the communication connection by the supervisor enables remote operation of the apparatus by the supervisor (Fig. 1). The merchant acquirer is separate from the merchant and the consumer; and therefore remote.

Claims 3-4, 9-12, 22-23, 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman as applied to claims 1 and 20 above, and further in view of Schneier.

In reference to claims 3 and 22, Spelman discloses encrypting working data transmitted over the channel (Fig. 1), However Spelman does not disclose authenticating the sender and receiver, resulting in an authorized sender and authorized receiver.

Schneier discloses a method of mutual authentication using the SKID, so that the sender and receiver know that they are talking to each other (page 54-57).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use mutual authentication as in Schneier in the system of Spelman. One of ordinary skill in the art would have been motivated to do this because the sender and receiver would be assured that they are talking to each other.

In reference to claim 4 and 23, a system is disclosed wherein the mapping module employs encryption in the mapping of working data in the domain to working data in the different domain such that the working data transmitted to the authorized receiver is anonymous data (column 6 lines 14-59).

In reference to claims 9 and 27, Spelman does not expressly disclose a system wherein the permanent storage means employs digital signatures on queried parts of the data to detect changes in data and thereby prevent tampering.

Schneier discloses a system of blind signatures where the document is signed and the person does not know what they are signing (pages 112-114). Digital signatures are used to detect changes in the data.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use blind signatures as in Schneier in the system of Spelman. One of ordinary skill in the art would have been motivated to do this because the person that signed the document can verify that they signed it, but will not know the contents of the document.

In reference to claims 10 and 28, Spelman discloses the concatenation of the encryption key and data (column 5 lines 42-54), however Spelman does not disclose digital signature is formed from a message digest.

Schneier discloses generating a message digest using a one-way hash and then signing the message digest (pages 38-39).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to sign a message digest as in Schneier in the system of Spelman. One of ordinary skill in the art would have been motivated to do this because it is a increases the speed of signing documents.

In reference to claims 11 and 29, Spelman does not disclose a system wherein the permanent storage means maintains a summary measure of stored data

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a summary measure of stored data in the system of Spelman. One of ordinary skill in the art would have been motivated to do this because it enable the reconstruction of data in the case of corruption of the original.

In reference to claims 12 and 30, Spelman does not disclose a system wherein said summary measure has a respective digital signature.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain a summary measure of stored data that has a digital signature in the system of Spelman. One of ordinary skill in the art would have been motivated to do this because it would enable the detection of changes to the summary measure.

Claims 13-15, 31-33, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman as applied to claims 1 and 20 above, and further in view of Ansell et al (6,151,631).

In reference to claims 13 and 31, Spelman does not expressly disclose storing a mapping table having cross-references between identifier portions of working data of the two domains

However Ansell discloses storing a mapping table (fig. 13 part 1306), the mapping table having cross-references between identifier portions of data of different domains (fig. 13 parts 1302 and 1304)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain mapping tables as in Ansell in the system of Spelman. One of ordinary skill in the art would have been motivated to do this because a mapping table organizes the information in a convenient manner.

In reference to claims 14, 32, and 38, Spelman does not disclose a system wherein the mapping module stores a mapping table for plural domains, the mapping table being formed of (i) an index section and (ii) a working reference section, the index section indicating identifier portion of working data in a first subject domain and the working reference section indicating corresponding identifier portion in a second domain, the working reference being encrypted, such that the mapping module performs decryption on a part of the mapping table to determine usable cross reference of the working data.

However Ansell discloses a system wherein the mapping module stores a mapping table for plural domains (Fig. 13 part 1306), the mapping table being formed of (i) an index section and (ii) a working reference section, the index section indicating identifier portion of working

data in a first subject domain and the working reference section indicating corresponding identifier portion in a second domain, the working reference being encrypted, such that the mapping module performs decryption on a part of the mapping table to determine usable cross reference of the working data (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain mapping tables as in Ansell in the system of Spelman. One of ordinary skill in the art would have been motivated to do this because a mapping table organizes the information in a convenient manner.

In reference to claims 15 and 33, Spelman does not disclose a system wherein the mapping module maps working data among plural domains.

Ansell disclose a system wherein the mapping module maps working data among plural domains (Fig. 13 part 1306).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to maintain mapping tables as in Ansell in the system of Spelman. One of ordinary skill in the art would have been motivated to do this because a mapping table organizes the information in a convenient manner.

Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman as applied to claim 1 above, and further in view of Coss et al (EP 0 909 074 A1).

Spelman discloses a system with a secure container (part 30 in Fig. 1); a computer system executing the communication module and the mapping module (part 30 in Fig. 1).

However Spelman does not disclose a firewall coupled to the computer system, the firewall being housed by the secured container so as to provide tamper-proof hardware.

Coss discloses a system with a firewall with the capability for supporting multiple domains (Page 4 paragraph 0025). Firewalls include tamper-proof hardware by definition.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to include a firewall capable of supporting multiple domains as in Coss in the system of Spelman. One of ordinary skill in the art would have been motivated to do this because firewalls prevent unauthorized access in computer networks.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Tuesday, March 29, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100